POLITIE

0 BD

Organisatieonderdeel Staf Korpsleiding
Afdeling Bestuursondersteuning
Team Juridische Zaken

Behandeld door
Functie
Bezoekadres Juliana van Stolberglaan 4-10
2595 CL Den Haag
Telefoon
E-mail

Retouradres: Postbus 17107, 2502 CC Den Haag)

Ons kenmerk
Uw kenmerk
Datum 16 juli 2013 **VERZONDEN 2 3 JULI 2013**
Bijlage(n) 0
Pagina 1/7

Ministerie van Veiligheid en Justitie
De heer mr. I.W. Opstelten
Postbus 20301
2500 EH Den Haag

Onderwerp Reactie KC op wetsvoorstel computercriminaliteit III

Geachte heer Opstelten,

In reactie op uw brief d.d. 2 mei 2013) bied ik u hierbij de reactie van de politie aan op het concept wetsvoorstel computercriminaliteit III.

De aanpak van cybercrime is al geruime tijd onderdeel van de landelijke prioriteiten die tussen de politie en het Ministerie van Veiligheid en Justitie zijn afgesproken. Daarnaast zorgt de toenemende omvang en ernst van cybercrime en high tech crime in het bijzonder, waarbij internet als instrument wordt ingezet, voor de noodzaak om de wet aan te passen. De politie is daarom verheugd met dit wetsvoorstel. De wet wordt daarmee aangepast aan de eisen van deze tijd.

Op dit moment werkt de politie samen met uw departement aan een opdrachtformulering voor een impactanalyse, waarmee de consequenties van het concept wetsvoorstel in kaart zullen worden gebracht. Hiermee moet voor de politie inzichtelijk worden in hoeverre dit wetsvoorstel gevolgen heeft voor de taakuitvoering van de politie en wat onder meer de personele, organisatorische en financiële gevolgen, de gevolgen voor ICT-systemen en administratieve lasten zijn.

In afwachting van de uitkomsten van de impactanalyse wil ik dan ook een voorbehoud maken op de consequenties die het concept wetsvoorstel computercriminaliteit III kan hebben op de politie. Deze zijn op dit moment nog niet te overzien. Met de uitkomsten van de impactanalyse dient gekeken te worden in hoeverre die passen binnen de huidige afgesproken kaders dan wel meegenomen dienen te worden in nog op te stellen toekomstige kaders. Hierover wil ik zo spoedig mogelijk na het opleveren van de impactanalyse met uw departement in overleg.

Los van dit voorbehoud wordt hierna de reactie van mijn korps in volgorde van onderwerp van uw brief weergegeven.

1. Onderzoek in geautomatiseerd werk

<u>1a. *Herdefinitie Geautomatiseerd Werk*</u>
Door de voortschrijdende techniek en het steeds verder integreren van verschillende functionaliteiten in één apparaat, is de huidige definitie in zijn algemeen niet langer houdbaar. Hierdoor kwam zowel de strafrechtelijk bescherming van geautomatiseerde werken als de bepaalbaarheid van de grenzen van bevoegdheden in het gedrang. Bij de politie werd al langer nagedacht over een herdefiniëring van het concept ´computer´, maar het blijkt lastig om een definitie te vinden die in de meeste gevallen

POLITIE

aansluit bij het maatschappelijk gevoel over wat nog wel en wat niet meer moet worden beschouwd als een 'computer'. De politie kan zich vinden in de voorgestelde definitie omdat die beter aansluit bij de maatschappelijke beleving van nu en een uitsluiting van (bepaalde typen) apparaten van de definitie voorkomt waardoor daaraan de strafrechtelijke bescherming zou worden onthouden die dergelijke (typen) apparaten gezien hun maatschappelijke context wel verdienen. De politie is, gezien de snelle ontwikkelingen op dit terrein, vermoedelijk met u, wel benieuwd naar de duur van de houdbaarheid van deze definitie.

1b. *Artikel 125ja Sv - De bevoegdheid tot het binnendringen in geautomatiseerde werken*
Doorzoeking / Onderzoek in een geautomatiseerd werk. Het bevel 125ja Sv en aanpassing daarvan
De wisselwerking tussen een uit te voeren hoofdbevoegdheid en de daaraan ondersteunende bevoegdheid tot binnendringen in een geautomatiseerd werk kan in voorkomende gevallen complex zijn. De kans op dergelijke complexiteit wordt groter indien sprake is van een al lopend onderzoek, waarin reeds bevoegdheden (zoals bijvoorbeeld afluisteren vertrouwelijke communicatie) worden toegepast. Het maakt de uitvoerbaarheid van toepassing van deze bevoegdheid beter nu de mogelijkheid geboden wordt beide bevelen 'ineen te schuiven'. Hierdoor zijn de aspecten van beide bevoegdheden beter in onderling verband te bezien en te motiveren.
Tevens positief is dat nu reeds rekening is gehouden met het feit dat men bij het uitvoeren van deze bevoegdheid zaken kan tegenkomen die nopen tot verandering van de eerdere plannen of dat gedurende de looptijd de situatie zelf verandert, waardoor een verschuiving plaatsvindt in de noodzakelijk onderzoekhandelingen. De mogelijkheid tot het geven van een mondeling bevel tot aanpassing geeft daarbij optimaal ruimte in te spelen op (acute) veranderingen binnen het onderzoek.
Terecht wordt (in paragraaf 2.6 en de artikelsgewijze toelichting) een voor het binnendringen in geautomatiseerde werken zorgvuldige voorbereiding vereist; deze staat in het wetsvoorstel dan ook op het hoogst mogelijke niveau. Voor eerste uitvoering vinden derhalve op verschillende niveau's maar liefst vier toetsmomenten plaats.

1c *Inperking bevoegdheid 125ja Sv 'bij verdachte in gebruik'*
In lid 1 van het voorgestelde artikel 125ja Sv wordt de inzet van deze bevoegdheid beperkt tot systemen 'bij verdachte in gebruik'. Hoewel de bedoeling wel kan worden gevolgd, is de wijze waarop daaraan wordt vormgegeven, ongelukkig. Tegen een aldus geformuleerde inperking bestaan de volgende bezwaren.
Hoewel de voorgestelde bevoegdheid buiten de 'BOB-titels' van het Wetboek van Strafvordering is geplaatst vertoont de bevoegdheid daarvan wel veel kenmerken. In de BOB-wetgeving zijn bevoegdheden normaal gesproken niet beperkt tot alleen verdachten.
Reeds in een titel IVa, een onderzoek naar een concreet geval met een concrete verdenking, bestaan al mogelijkheden tot toepassing van BOB-bevoegdheden op anderen dan alleen verdachte, ook als de toepassing van deze bevoegdheid een significante inbreuk op rechten vormt.
In de daaropvolgende titels wordt dit zelfs uitgebreid naar 'groepen personen'.
De beperking die bij toepassing van al die bevoegdheden geldt is dat bij het eindoordeel of de bevoegdheid daadwerkelijk zal mogen worden ingezet moet zijn voldaan aan de vereisten van proportionaliteit en subsidiariteit. De opsporings- en rechtspraktijk heeft inmiddels ruime ervaring met het toepassen van deze criteria als controle en rem op (te ongebreidelde) toepassing van (zware) dwangmiddelen. Het extra vereiste 'bij verdachte in gebruik' breekt met het bekende systeem en zal

POLITIE

daardoor in de opsporingspraktijk voor de nodige onduidelijkheid en discussie gaan zorgen.
Het bovenstaande punt wordt mede versterkt door het feit dat de door de minister voorgestelde beperking 'bij verdachte in gebruik' op vele wijze kan worden gelezen. Als de nauwe uitleg gevolgd wordt, zou de bevoegdheid niet gebruikt kunnen worden, terwijl de opsporing daar wel behoefte aan heeft. Denk daarbij aan het voorbeeld dat een verdachte een gebruiker/verzamelaar van kinderporno is en alleen woont. Hij(/zij) heeft al wel een tijdje een LAT relatie. Als de verdachte bij hem of haar op bezoek is, raadpleegt die verdachte wel een enkele maal zijn/ haar webmail of een andere site op de computer van verdachte. Gezien het sporadisch gebruik heeft die relatie geen eigen gebruikersaccount. Bij een te nauwe uitleg van de term 'bij verdachte in gebruik' zou in dit geval deze bevoegdheid niet toegepast kunnen worden.

Voor de politie is het mogelijk lastig uitvoering te geven aan het onderzoek zolang niet vaststaat wat 'bij verdachte in gebruik' ongeveer inhoudt. Stel dat verdachte met een boekhoudpakket zijn criminele boekhouding bijhoudt in de cloud, is dan op basis van deze bevoegdheid de politie gerechtigd tot het binnendringen in het gedeelte dat aan verdachte kan worden gekoppeld (voorzover mogelijk?) of mag de politie het dan ook van de andere kant benaderen door eerst het volledige netwerk van geautomatiseerde werken binnen te dringen (bijvoorbeeld de servers in de cloud die te relateren zijn aan het gebruik van dat boekhoudpakket) om vanaf daar te proberen het account van de verdachte te identificeren en binnen te komen, zodat de data kan worden veiliggesteld?).
De conclusie van al bovenstaande is dat de politie er voorstander van is dat de zinsnede 'bij verdachte in gebruik' uit de voorgestelde wettekst wordt geschrapt. Voor de inperking van de inzet van de bevoegdheid kan dan worden vertrouwd, net als bij de BOB-bevoegdheden, op de correcte toepassing van de beginselen van proportionaliteit en subsidiariteit. Deze beginselen worden dan in de besluitvorming of deze bevoegdheid toegepast mag worden getoetst door zowel, de officier van justitie, de CTC, de Procureur-Generaal en de rechter. Naar het oordeel van de politie is dat een afdoende bescherming van de belangen van de verdachte. Het niveau van toetsing ligt immers op het allerhoogste niveau.

1d *Afsluiten uitvoering bevel 125ja Sv*
Op pagina 27 van de concept memorie van toelichting wordt het uitgangspunt beschreven dat na afsluiting van het onderzoek in het geautomatiseerde werk dat geautomatiseerde werk in alle gevallen zo veel mogelijk moet worden achtergelaten in de oorspronkelijke staat.
Deze opdracht tot het zoveel mogelijk terugbrengen van het geautomatiseerde werk in oorspronkelijke staat wordt door de politie zo gelezen dat wordt bedoeld: Het systeem zoveel mogelijk achterlaten als ware de bevoegdheid nooit toegepast.

1e *Toepassing 125ja Sv ten behoeve van verkrijging locatiegegevens / Stelselmatige Observatie*
In de opsporing is het vaak van belang om te weten waar voor het onderzoek van belang zijnde personen zich 'ongeveer' bevinden. Niet zelden wordt daarbij gebruikt gemaakt van de bevoegdheid tot het stelselmatig observeren. Lang niet iedere observatie echter, zo blijkt uit uitgebreide jurisprudentie van de Hoge Raad, is zodanig inbreukmakend of stelselmatig dat daarvoor een bijzondere bevoegdheid voor dient te worden gehanteerd.
In voorkomende gevallen wordt gebruik gemaakt van, middels een bevel opnemen telecommunicatie (126m Sv serie), meekomende locatiegegevens. Deze gegevens maken deel uit van de standaard aan te leveren verkeersgegevens bij de uitvoering

POLITIE

van een tap-bevel. Deze locatiegegevens zijn van beperkte nauwkeurigheid en (natuurlijk) niet beschikbaar wanneer niet al een tap loopt.
Steeds meer apparaten communiceren niet alleen maar bevatten ook GPS of andere mogelijkheden tot (nauwkeurige) locatiebepaling. Deze -meer nauwkeurige- informatie maakt geen deel uit van de standaard aan te leveren gegevens. Daarnaast is het, wanneer met grotere precieze en enige duur en frequentie de locatie van een persoon of apparaat wordt bepaald (als expliciet opsporingsdoel) juridisch juister om gebruik te maken van een bevoegdheid die daar in het bijzonder voor is opgesteld door de minister (de 126g Sv serie).
Het wordt dan door de politie ook als positief ervaren dat de minister de mogelijkheid creëert om ook met toepassing van de voorgestelde bevoegdheid art. 125ja Sv van de in een geautomatiseerd aanwezige locatiegegevens gebruik te maken. Op deze wijze kan de politie per casus gebruik maken van het best passende middel.

<u>1f *Functiescheiding bij toepassing bevoegdheid*</u>
De uitoefening van de bevoegdheid van het voorgestelde artikel 125ja Sv wordt toebedeeld aan een 'technisch team' bij de politie dat op enige afstand staat van het team dat het daadwerkelijke opsporingsonderzoek uitvoert. Dit kan rekenen op de instemming van de politie.
Op deze wijze kan de bijzondere (en over meerdere personen verdeelde) expertise die noodzakelijk is om aan deze bevoegdheid in alle aspecten goed uitvoering te geven bij dit technisch team worden belegd en eenvoudiger het hoge niveau van expertise worden gehandhaafd dat voor een correcte uitoefening van de voorgestelde bevoegdheid noodzakelijk is.
Dit concept van functiescheiding heeft zich in de praktijk al bewezen als werkende methode om correct, vakkundig en zorgvuldig uitvoering te geven aan (zware) bevoegdheden; het wordt namelijk ook toegepast bij de uitvoering van onder meer de plaatsing van bakens op materiaal en voertuigen en bij de plaatsing van apparatuur ter uitvoering van een bevel opnemen vertrouwelijke communicatie. De wijze waarop hieraan bij deze bevoegdheden uitvoering wordt gegeven geeft zelden aanleiding tot vragen of discussie. Daardoor kan met behoorlijke zekerheid worden gezegd dat het concept ook voor de nieuwe bevoegdheid zal werken.

<u>1g *Logging*</u>
Aan het eind van paragraaf 2.4 van de concept memorie van toelichting schrijft de minister dat ten alle tijde moet kunnen worden gecontroleerd welke technische handelingen in het desbetreffende geautomatiseerde werk hebben plaatsgevonden, zodat op een later moment geen twijfel kan ontstaan over de aard en consequenties van de handelingen die zijn verricht bij de uitvoering van de bevoegdheid'. Daar is de politie het van harte mee eens.
Aan het eind van paragraaf 2.5 staat 'doordat alle technische handelingen die door de opsporingsambtenaren van het technische team worden verricht, worden gelogd en deze handelingen bovendien hun weerslag vinden in een proces-verbaal, is achteraf altijd controle mogelijk op de integriteit van de werking van het technische hulpmiddel en van de informatie die met behulp daarvan is vergaard. Op deze manier is het mogelijk om de ter terechtzitting gevoerde verweren over de integriteit van het verzamelde bewijsmateriaal te toetsen.'
De 'logging' zal dan betrekking hebben op vereisten van authenticiteit en integriteit die moeten garanderen dat de vastlegde inhoud correct is overgenomen en niet beschadigd of gemanipuleerd is. Dit stuit vanuit de politie dan ook op geen enkel bezwaar.

POLITIE

De politie is er echter wel voorstander van dat de wijze van beoordeling van de methode plaats zal vinden op een zodanige wijze dat de opsporingsmethode niet direct openbaar gemaakt wordt. Ook nu hoeft de methode, dat wil zeggen de inzet van technische hulpmiddelen bij de uitvoering van reeds bestaande bijzondere opsporingsbevoegdheden niet geopenbaard te worden. Er is immers een besluit technische hulpmiddelen waarin zeer strenge eisen zijn opgenomen ten aanzien van de middelen die worden ingezet. Zonder die keuring mogen die middelen niet ingezet worden.
Het is voor de opsporing van groot belang dat het zijn methodieken niet te hoeft prijs te geven, zodat ze in de toekomst ook nog inzetbaar zijn. Dat is van belang omdat het ontwikkelen veel menskracht en tijd kost. Daarnaast is de veiligheid van het politiesysteem in het geding.

2. Ontoegankelijkmaking van gegevens / Notice-and-Takedown
De thans voorgestelde regeling is naar de mening van de politie een duidelijke verbetering ten opzichte van de huidige situatie.
Ondanks de te waarderen opstelling van de partijen, aangesloten bij de gedragscode Notice-and-Takedown, is het goed dat er nu een meer reguliere wettelijke regeling komt ten aanzien van de ontoegankelijkmaking van gegevens. Deze neemt een hoop bezwaren omtrent de toepassing van dit middel weg.
Een van de belangrijkste daarvan is dat de overheid bij het offline halen van strafbare uitingen of gegevens niet langer afhankelijk is van medewerking van beschikkingsmachtigen die, in feite, vrijwillig is. Dat een rechterlijke controle nu onderdeel uitmaakt van de bevoegdheidstoepassing is een goed werkbare situatie.

In het kader van de noodzakelijke snelheid bij het tegengaan van (actuele) uitingsdelicten merkt de politie op dat zeker bij verspreiding van informatie op het internet zaak is eerder binnen uren dan dagen te reageren. Duurt het namelijk langer, dan is dergelijke content vaak al overgenomen door andere partijen. De ervaring leert dat op dat moment de kans op succesvolle ontoegankelijkmaking is verkeken. Hoe meer daarna nog geprobeerd wordt dit alsnog te bewerkstelligen, hoe groter de daadwerkelijke verspreiding en de (media)aandacht voor de betreffende content.
In de toelichting (en niet in het wetsartikel zelf) wordt de vrijwillige gedragscode als primaire methode aangewezen (in paragraaf 3.2).
Als men alvorens een bevel af te mogen geven eerst moet wachten of de aangeschreven beschikkingsmachtige gehoor gaat geven aan een verzoek, gaat in sommige gevallen kostbare tijd verloren. Tijd die zowel het onderzoek vertraagt als ongewenste gevolgen kan hebben.
De politie is er voorstander van dat de vrijwillige regeling naast de bevoegdheid kan bestaan zonder onderlinge prioritering. Een bevel als er zeer veel haast is en de vrijwillige regeling als er daar ruimte voor is.

3. Decryptiebevel aan verdachte
In paragraaf 4.1 van de concept memorie wordt melding gemaakt van het feit dat er software bestaat met als specifieke doel het ondermijnen van forensisch onderzoek. Ook wordt gesteld dat encryptie vooral wordt gebruikt binnen bepaalde netwerken van kinderpornogebruikers en verspreiders.
De tekst van de memorie moet niet zo gelezen worden dat in zijn algemeenheid encryptie / versleuteling iets is, dat alleen of voornamelijk wordt gehanteerd door criminelen.
De politie benadrukt dat zij zich ervan bewust is dat encryptie niet alleen gebruikt wordt voor criminele doeleinden, maar veelal ook voor legale. Er is ook geen of nauwelijks onderscheid tussen de gebruikte software voor beide doeleinden.

POLITIE

De politie zelf maakt gebruik van versleuteling bij (transport van) gevoelig materiaal. Banken maken gebruik van versleuteling (op de verbindingen) om veilig internetbankieren mogelijk te maken. Security-bewuste bedrijven passen versleuteling toe op hun klantgegevens, zodat in geval van een succesvolle inbraak op hun geautomatiseerde werken in ieder geval de klant daarvan niet de dupe is. Van versleuteling is de politie in alle genoemde gevallen een voorstander.
Sterker nog, de politie moedigt burgers en bedrijven aan hun systemen en gegevens goed te beveiligen door besturingssystemen en programma's actueel te houden, gebruik te maken van beveiligde verbindingen voor belangrijke zaken en zelfs door gegevens te versleutelen, zodat zelfs wanneer een cybercrimineel weet binnen te komen hij weinig of niets van waarde aantreft op het binnengedrongen systeem.
Het enkel aanwezig hebben van versleutelingsoftware of versleutelde gegevens is op zich geen reden van verdenking. Het feit dat gebruik wordt gemaakt van versleutelingssoftware met ingebouwde 'plausibledeniability' doet daaraan niets af. Indien er sprake is van een verdenking is deze altijd (mede) gebaseerd op andere feiten.
Het opsporen van misdrijven waarin digitale componenten een rol spelen is een toenemende factor in het politiewerk. De politie waardeert dat de minister bij de meest in het oog lopende problemen daarbij de politie de helpende hand toesteekt door het creëren van nieuwe bevoegdheden zoals die van het voorgestelde artikel 125ja Sv en het onderhavige bevel dat de politie moet helpen in de strijd tegen criminelen die gebruik maken van encryptie om de politie het opsporen moeilijk te maken.

4. 'Stelen' en 'Helen' van gegevens
Gezien het feit dat in de moderne maatschappij gegevens qua belang inmiddels steeds meer gelijk komen te liggen met het fysieke komt aan gegevens, naar de mening van de politie, een gelijkwaardige bescherming toe als goederen. De politie is dan ook blij met het feit dat zowel het 'stelen' als het 'helen' van gegevens in dit conceptwetsvoorstel terugkomen.

De politie wil, in aanvulling op de toelichting van het wetsvoorstel, benadrukken dat het kwalijke van het 'stelen' van gegevens niet alléén gelegen is in de verspreiding daarvan via internet. Het maakt in principe werkelijk niet uit of die verspreiding via internet makkelijker zou zijn geworden. Ook de diefstal van gegevens die niet verspreid of openbaar worden gemaakt aan grote groepen mensen (juist zelfs bewust in kleine kring worden gehouden) kunnen zeer schadelijk zijn.

In de opsporingspraktijk, vooral bij onderzoeken naar computercriminaliteit, worden nogal eens grote hoeveelheden gegevens aangetroffen, waar -gezien de plaats waar ze worden aangetroffen- geen redelijke verklaring voor is. Wat moet immers iemand die geen (web)winkel heeft met de creditcardgegevens van honderden, zo niet duizenden mensen.
Wat is de reden van het hebben van een lijst van duizenden mailaccounts met bijbehorende wachtwoorden? Waarom heeft iemand de toegangsgegevens van honderden PayPal accounts?
Ook op dit moment is dit natuurlijk allemaal al uiterst verdacht (in de maatschappelijke zin van het woord), maar strafrechtelijk gezien bieden dergelijke dataverzamelingen thans geen overmaat aan aanknopingspunten voor vervolging.
De politie is het zeer eens met dit onderdeel van dit wetsvoorstel.
Dit betekent bijvoorbeeld dat ook wanneer hackers niet betrapt kunnen worden tijdens het hacken en/ of overnemen van gegevens, zij alsnog strafvorderlijk kunnen worden aangepakt voor hun activiteiten.

POLITIE

Hetzelfde geldt voor al dan niet professionele tussenhandelaren die bijvoorbeeld op grote schaal (via botnets) verzamelde betaalgegevens (tegen winst) door verhandelen aan organisaties met de mogelijkheid deze gegevens te gelde te maken en/of wit te wassen.

Tot slot wil de politie op dit punt kwijt dat zij ook positief kijkt naar de formulering van het voorgestelde artikel 139f , lid 2 Sv. Bij deze wijze van formuleren lijkt voldoende rekening te zijn gehouden met de ontwikkelingen in de moderne (gedigitaliseerde) maatschappij waarbij het openbaar maken van feiten met nieuws- of maatschappelijke waarden niet langer voorbehouden is aan 'klassieke journalisten'.

4.1 Helen en stelen van gegevens / identiteitsdiefstal
De politie is er voorstander van dat in dit wetsvoorstel ook een strafbaarstelling van het 'stelen' van een (digitale) identiteit wordt opgenomen. In feite speelt daar hetzelfde probleem als bij gegevens.
Weliswaar zijn veel van de noodzakelijke handelingen om een (digitale) identiteit succesvol te stelen, of te gebruiken, strafbaar gesteld, maar de daad van het 'overnemen' of voorhanden hebben van dergelijke informatie daarvoor niet. Hetzelfde geldt voor het enkel (daadwerkelijk) aannemen van een valse (digitale) identiteit (te onderscheiden van een pseudoniem of nickname).

In een steeds verder digitaliserende wereld waarin contacten steeds minder plaatsvinden tussen mensen die elkaar in 'real life' kennen en waarin de snelheid van het handelsverkeer steeds minder ruimte biedt voor uitgebreide controles van diverse zaken, is het met de juiste set gegevens in handen niet al te ingewikkeld meer om je voor te doen als een ander en met die identiteit dan je voordeel te doen.
Een goed voorbeeld hiervan is het stelen van Paypal 'credentials' waarmee de crimineel op naam van een ander allerlei makkelijk te herverhandelen goederen aanschaft. Vervolgens kunnen er drie dingen gebeuren. Of de echte 'eigenaar' van die identiteit draait op voor de schade, of de tussenpersoon (in dit geval Paypal omdat zij dit aan haar klanten garandeert) of in sommige gevallen de leverancier, omdat de tussenpersoon met succes zijn geld weet terug te halen. Degene die er het minst last van heeft is gemiddeld gezien de crimineel. De politie is er voorstander van identiteitsdiefstal alsnog in het wetsvoorstel op te nemen.
Overigens is de politie op de hoogte van het reeds door de Tweede Kamer behandelde en aangenomen amendement van het lid Dijkhoff c.s. (Kamerstuk 33352, nr. 7) d.d. 5-7-2013 waarin het gebruik van die gegevens strafbaar wordt gesteld.

De politie is blij met de voorgestelde wetswijzigingen en heeft deze wijzigingen nodig om haar taak te kunnen blijven uitvoeren. Tevens wordt hiermee een belangrijke lacune in de opsporing, onstaan door de zeer snelle ICT-ontwikkelingen, gedicht.

Met vriendelijke groet,

korpschef